In Cloud We Trust—When It Is Secured

A point of view paper on the importance of security for cloud-based computing

Abstract

Cloud computing is dynamically changing the way companies do business, as well as how customers access their offerings. The massively scalable IT-enabled capacities of the cloud have given it universal appeal. But there may be a price to pay for the convenience. Even as they embrace the cloud to help them transform their business, companies have critical security concerns such as data loss, privacy, cyber attacks, and unauthorized access. This paper suggests building a security framework specific to a cloud-based environment by which companies can manage the security of their data and protect it from attack. Knowing that they can manage the risks associated with the cloud will give companies the ability to take advantage of its many benefits.

Introduction

Cloud computing is changing the rules of the information technology game. The technology is sweeping across business sectors and changing the way companies do business as well as the way customers access data, services, and applications. The National Institute of Standards and Technology (NIST), part of the US Department of Commerce, describes cloud computing as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”¹ A new disruptive technology such as cloud computing comes with its associated risks. While some of these risks are similar to those in the traditional service provision model, others are unique to cloud computing.

Top Cloud Security Concerns

As cloud computing is an externally provided service, many organizations are playing the waiting game and hoping the technology, along with the service models and the associated security features, is mature enough before they adopt it. While their concern is natural, as with any service, enterprises can assess the associated risks and vulnerabilities with cloud computing and take the necessary measures to mitigate them.

When data is stored in a cloud, whether private, public, or hybrid, there are bound to be concerns about privacy, compliance, and governance. Privacy concerns include questions of security and whether your competition or malicious users can access sensitive company or customer data. If confidential data is being consumed or accessed by people outside the organization, it is vulnerable to data fraud and other complications.

As with traditional IT service providers, enterprises expect cloud service providers (CSPs) to conform to their stringent security audits and certifications. Compliance is an important feature of security. Enterprises should let their CSPs know the parameters they will be evaluated and audited against. The providers should also be held accountable by regulatory agencies to ensure compliance with the most stringent controls and measures.

Governance is a key challenge. Enterprises worry about data ownership and what privileges (such as access, update, and delete) users may have when processing their data. Different deployment models present different governance issues.

The differences in scope and control between the cloud consumer and cloud provider are illustrated in Figure 1. The arrows in the diagram denote the approximate range of the cloud provider’s and the consumer’s control over the cloud environment for each service model. In general, the level of support available from a cloud provider and the scope and control of the cloud consumer are inversely proportional. This implies that the higher the level of support available from a cloud provider, the more narrow the control the consumer has over the system.

It is essential that enterprises understand these issues associated with a cloud deployment in order to effectively manage the security of their data.

Enterprises need to evaluate the security of their data and the effectiveness of their security features against phishing and other cyber-attacks. Corporate and customer data security is an important consideration irrespective of whether the data is managed by the organization itself or by a third-party CSP. It is important to monitor the safety and the various steps taken by the provider to protect the data from cyber as well as natural or physical attacks.

Building a Cloud Security Framework

Security features are likely to be implemented in several layers. A combination of physical, network, system, and application security features will promote confidence in the cloud.

The security requirements of applications managed in traditional, on-premise data centers are very different from those in the cloud environment. In such an environment, the management and maintenance of the security policies, processes, and controls are the joint responsibility of many stakeholders. The CSP, service consumer, cloud broker, cloud auditor, and other parties are all responsible for the data security in such a set-up.

An effective cloud security framework can be built by adding policies, procedures, standards, and regulatory requirements specific to a cloud environment, alongside those that already exist.

Cloud computing also requires service management, governance, planning, and lifecycle management. These are the building blocks of a comprehensive and secure cloud architecture.

The cloud security framework explained in Figure 2 addresses the concerns and challenges discussed above. It also shows the measures that will increase confidence levels for users of cloud services.
Benefits of a Secure Cloud

While security concerns are legitimate and require attention, they should not mask the fact that cloud computing has the potential to significantly improve the security of a company’s information and data platforms.² Implementing cloud security strategies and policies can help achieve a range of benefits.

The ability to scale or re-allocate resources on-demand to filter, optimize traffic, and encrypt—has clear advantages. It allows the provider to improve security if an attack is likely or is under way and this improves businesses continuity.

Most cloud providers offer a standardized and compatible interface to their customers’ outsourced managed security services (MSS) providers. Cloud providers may look at adding security services to their portfolio, allowing customers to switch MSS providers seamlessly with low set-up costs.

By pooling and concentrating resources, cloud providers can offer their customers several benefits including the lower cost and easy application of a comprehensive security policy. Data management becomes easier, as do the processes of troubleshooting, managing incidents, and maintaining processes and systems.

'Infrastructure as a Service' (IaaS), one of the key features of cloud computing, offers other benefits allied to security. In the event of a security attack, an image of a live virtual machine can be created and used for forensic analysis. This minimizes the downtime needed for analysis. Multiple clones can be created in parallel using on-demand storage. The result is effective security incident analysis for better tracking and preventive measures for the future. Cloud-based security logs for auditing purposes can be scaled up dynamically, and this helps meet the increasing demand for security logging without impacting performance.

Conclusion

Critical security concerns such as data loss, privacy, cyber threats, vulnerability, and unauthorized access are significant barriers for enterprises considering cloud computing. Cloud providers that can address these concerns and build a reputation for security can differentiate themselves and provide significant value to their customers. Effective security requires the addition of features that are specific to a cloud-based IT environment. The framework described here provides a basis for development and will allow providers to accrue other allied benefits.

So in the same way that we say, “In God we trust, but we keep our cars locked”, cloud computing offers significant enterprise benefits which will be best achieved with the added comfort of a robust security framework.

About the Authors

Dr. C. Parthiban
Solution Manager

Dr. C. Parthiban is a Solution manager in the Global Consulting Practice – Business Incubation Solutions group at Tata Consultancy Services (TCS). He has 15 years’ experience covering a wide range of areas including IT strategy, Infrastructure Optimization, Architecture Solutions, and Systems Integration, and has led large consulting engagements. He holds a doctorate in Applied Science from Anna University, in Chennai, India.

Priyambad Pattanayak
Infrastructure Consultant

Priyambad Pattanayak is an Infrastructure Consultant in TCS’ Global Consulting Practice – Business Incubation Solutions group. He has over eight years of experience in the IT industry covering a wide range of areas including IT Strategy, Cloud Strategy Assessment, Benchmarking, and Business Continuity.
About TCS’ Global Consulting Practice

TCS’ Global Consulting Practice (GCP) is a key component in how TCS delivers additional value to clients. Using our collective industry insight, technology expertise, and consulting know-how, we partner with enterprises worldwide to deliver integrated end-to-end IT enabled business transformation services.

By tapping our worldwide pool of resources – onsite, offshore, and near-shore – our high caliber consultants leverage solution accelerators and practice capabilities, balanced with our knowledge of local market demands, to enable enterprises to effectively meet their business goals.

GCP spearheads TCS’ consulting capacity with consultants located in North America, UK, Europe, Asia Pacific, India, Ibero-America, and Australia.

Contact
For more information about TCS’ Global Consulting Practice
visit: http://www.tcs.com/consulting
Email: global.consulting@tcs.com

About Tata Consultancy Services Ltd (TCS)
Tata Consultancy Services is an IT services, consulting and business solutions organization that delivers real results to global business, ensuring a level of certainty no other firm can match.

TCS offers a consulting-led, integrated portfolio of IT and IT-enabled infrastructure, engineering and assurance services. This is delivered through its unique Global Network Delivery Model™, recognized as the benchmark of excellence in software development. A part of the Tata Group, India’s largest industrial conglomerate, TCS has a global footprint and is listed on the National Stock Exchange and Bombay Stock Exchange in India.

For more information, visit us at www.tcs.com

IT Services
Business Solutions
Consulting